

PaperCut Konica Minolta i-Option Embedded Manual

Contents

1	Which version do I install?	4
2	Device Type Compatibility	5
3	Overview	6
3.1	Consistency	6
3.2	Integration	6
3.3	Rate of development	6
3.4	Vendor Neutral	7
3.5	Security	7
4	Installation	8
4.1	Konica Minolta i-Option Device Compatibility	8
4.1.1	MFD Compatibility	8
4.2	Requirements	9
4.3	Setup Procedure	10
4.3.1	Configure OpenAPI Settings	10
4.3.2	Web Browser Configuration	12
4.3.3	Enabling Unauthenticated Printing	13
4.3.4	Additional Device Hardware Settings	14
4.3.5	PaperCut Settings	14
4.3.6	Verify Device Creation	15
4.3.7	Additional Network Security (optional)	18
4.4	Upgrading to a newer version	18
5	Post-install testing	19
5.1	Test Preparation	19
5.2	Scenario 1: Standard copying	20
5.3	Scenario 2: Copying with account selection	22
5.4	Scenario 3: Print release	24
5.5	Scenario 4: Scanning and faxing	27

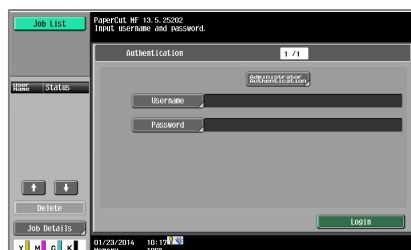
6	Configuration	29
6.1	Device Function	29
6.2	Authentication Methods	30
6.3	Customizing Text and Messages.....	31
7	Advanced Configuration	32
7.1	Config Editor	32
7.2	Setting an explicit PaperCut Server Network Address	40
7.3	Configuring Swipe Card Readers	41
7.4	Card Self-Association	44
7.4.1	Self-Association Workflow.....	44
7.5	Host-based authentication.....	45
7.6	Customizing the Header Logo.....	45
7.7	Customizing the Header Colors	45
7.8	Customizing the Application Logo Icon	46
8	Uninstalling	47
9	Known Limitations and Security	47
9.1	Combining Auto-color and Duplex	47
9.2	Copy restrictions on restricted accounts.....	47
9.3	PageScope Box Operator PC software	47
9.4	Job logging in case of network outages or firmware defects.....	47
9.5	Account Selection and Print Release.....	48
9.6	Bypassing the System	48
9.7	Release All Device Configuration is Always Shown	48
9.8	Browser Resetting to the Connection Screen	48
9.9	Browser screen appears with scroll bars.....	49
9.10	Browser SSL Certificate Installation.....	49
9.11	Browser and connection errors.....	50
10	FAQ & Troubleshooting	51

This manual covers the PaperCut MF Konica Minolta i-Option embedded setup. For general PaperCut MF documentation, please see the [PaperCut MF manual](#).

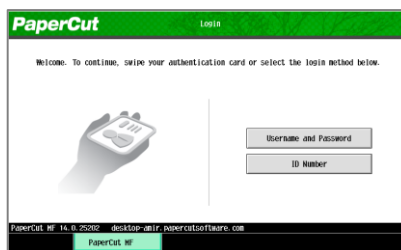
For Konica Minolta MFDs not configured to use the i-Option, please refer to the [PaperCut MF Konica Minolta Standard UI Embedded manual](#).

1 Which version do I install?

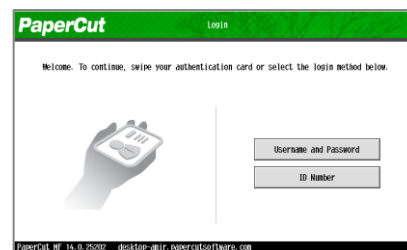
Standard UI



i-Option OpenAPI 3



i-Option OpenAPI 4



Comparison Matrix

	Standard UI	i-Option OpenAPI 3	i-Option OpenAPI 4
Login with username/password, ID and card.	✓	✓	✓
Monitoring and control of copying scanning and faxing.	✓	✓	✓
Release jobs from a hold / release queue	✓	✓	✓
Secure access to device functions	✓	✓	✓
Account invoice and comment option	✗	✓	✓
Customizable logo and colors	✗	✓	✓
Customizable print release and account selection screens	✗	✓	✓
Release prints on login	✗	✓	✓
Card self-association during login	✗	✓	✓
Automatic SSL certificate installation	✗	✗	✓
Full screen display	✗	✗	✓
Logged on username display	✗	✗	✓

Type

Konica Minolta i-Option (OpenAPI 3.1+) ▼

Type

Konica Minolta i-Option (OpenAPI 3.1+) ▼

Type

Konica Minolta i-Option (OpenAPI 4.0+) ▼

Standard UI Requirements:

- Available on OpenAPI 3 and OpenAPI 4 devices with a hard drive installed

i-Option OpenAPI 3 Requirements:

- Available on OpenAPI 3 and OpenAPI 4 devices with a hard drive installed
- LK101 upgrade kit required from Konica Minolta
- NetFront or WebKit browser depending on MFP model

i-Option OpenAPI 4 Requirements:

- Available on OpenAPI 3 and OpenAPI 4 devices with a hard drive installed
- LK101 upgrade kit required from Konica Minolta
- NetFront or WebKit browser depending on MFP model
- Currently available in Australia & Europe only

2 Device Type Compatibility

Device type in PaperCut MF	i-Option UI Supported	Standard UI Supported	Notes
Konica Minolta (OpenAPI 2.3+)	No Use Other Embedded Manual	Yes Use Other Embedded Manual	Consider upgrading your device to newer OpenAPI/firmware.
Konica Minolta (OpenAPI 3.1+)	Yes MFD Upgrade may be required.	Yes Use Other Embedded Manual	Web browser UI automatically selected for new devices if MFD supports i-Option. Standard UI can be enabled through PaperCut configuration.
Konica Minolta (OpenAPI 4.0+)	Yes MFD Upgrade may be required.	Yes Use Other Embedded Manual	Web browser UI automatically selected for new devices if MFD supports i-Option. Standard UI can be enabled through PaperCut configuration. OpenAPI 4.x mode is currently supported on Australian and European devices only.

3 Overview

This manual provides an overview of the installation, configuration and operation of PaperCut's embedded software MFD (Multi-Function Device) solutions. Today's MFDs are smarter – they have touch screens and offer the ability to run applications directly on the device. The goal of PaperCut Software's embedded MFD solution is to leverage these smart devices and to provide walk-up copier users with the same set of rich application features provided in the print control area. These include:

- Secure access to device functions
- End user authentication including integration with single sign-on environments
- Monitoring and control of photocopying, scanning and faxing (quotas, charging, allocation and logging)
- Allocation of copying, scanning and faxing to accounts/departments/cost-centers/projects
- Release jobs from a hold/release queue (Secure & Find Me Printing)
- Group based access control: Limit access to color copying, the device as a whole, or to selected user groups
- Self-associate swipe cards with domain user accounts directly at the device
- Streamlined interface throughout
- Self-association and print release are possible as part of the device login
- Account invoice and comment options are supported
- Customizability of print release and account selection screens
- Logo, messages and colors are customizable

Highlights of the embedded solution include:

3.1 Consistency

The embedded solutions are developed in-house by the PaperCut Software development team. This ensures that the copier interface is consistent with the workstation print interface, meaning users only have to learn one system.

3.2 Integration

PaperCut is a single integrated solution where print, internet and copier control are all managed in the one system. Users have a single account and administrators have the same level of reporting and administration for all services. The embedded solution interacts with the PaperCut server using a Service Oriented Architecture (SOA) and web services based protocols.

3.3 Rate of development

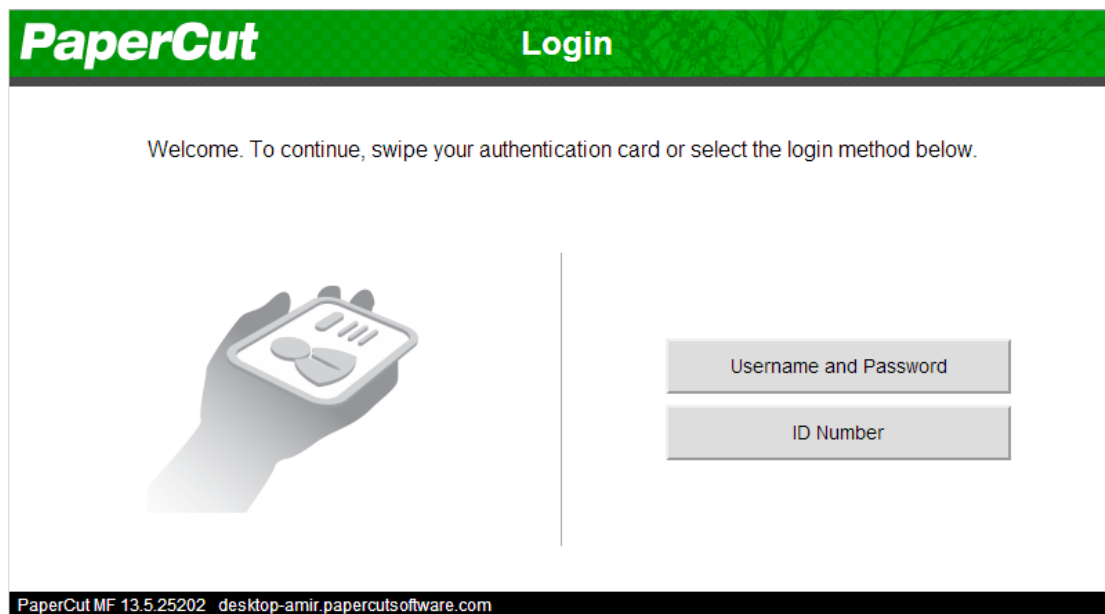
PaperCut is developed under a release-often policy where new features are made available to users as soon as they are complete. Unlike hardware based solutions, new versions can be delivered to users as regularly as software updates.

3.4 Vendor Neutral

PaperCut remains true to its vendor neutral stance. All embedded solutions are equal and support all server OS's including Windows, Linux and Mac.

3.5 Security

A large percentage of PaperCut's user base is in educational environments where security is important. All embedded solutions are developed with security in mind. Where security objectives cannot be satisfied, the deficiencies are fully disclosed.



The Konica Minolta onboard/embedded application login screen example

4 Installation

This section covers the installation of the PaperCut embedded application for compatible Konica Minolta MFDs. The embedded application will enable MFD access control, secure printing and “Find-Me” printing, and allow logging and control copying, scanning and faxing.(for information on just tracking network printing see the PaperCut user manual).

4.1 Konica Minolta i-Option Device Compatibility

The PaperCut MF Konica Minolta i-Option device type is available as either an OpenAPI 3.x or OpenAPI 4.x capable device type, and you should select the correct device type for the physical device you have.

Note that an OpenAPI 4.x device can still use PaperCut’s OpenAPI 3.x configuration; however with the following feature omissions.

- Full screen UI mode, to maximize the size of the UI displayed
- Automatic SSL certificate registration on the device
- Current username display when logged on to the device

The embedded software will automatically detect if i-Option is supported by the MFD and run with i-Option (web browser UI) as a preference, where i-Option is not supported it will continue to run using Konica Minolta standard UI screens. Automatic browser selection will be skipped for any existing devices on upgrade unless explicitly set through configuration, for details see section 4.4.

4.1.1 MFD Compatibility

PaperCut embedded i-Option supports any multi-function browser capable Konica Minolta device with “OpenAPI” 3.1+ and a hard drive installed.

Such a device must have the i-Option license installed in the form of an LK101 upgrade kit from Konica Minolta.

Refer to: http://www.biz.konicaminolta.com/solutions/i_option/#SPECIFICATIONS

NOTE: The following devices also require additional memory when running OpenAPI applications (like PaperCut), please contact Konica Minolta for information:

- Bizhub C203\C253\C353\C451\C550\C650

i-Option is supported via two web browsers that are available on the MFD. The interface will vary slightly depending on the browser type used.

The browsers are implemented depending on the MFD model as follows:

- NetFront Browser is implemented on the following models: C650, C550, C451/C353, C253, C203/751, 601/501, 421, 361/C652, C552, C452/C652DS, C552DS/C360, C280, C220/423, 363, 283, 223/602, 502, 652, 552.

- WebKit Browser is implemented on the following models; C754, C654/C554, C454, C364, C284, C224/754, 654/C554e, C454e, C364e, C284e, C224e.

OpenAPI 4 devices are currently not available on MFDs in all regions. Your Konica Minolta regional Head Office will be able to advise you on the timeframes for OpenAPI 4 availability in your area.

Devices with OpenAPI 4.x or later provide additional benefit of being able to run in full screen browser mode, to maximize the size of the UI displayed; as well as supporting automatic SSL certificate registration on the device.

Displaying currently logged on user in the message area of the screen is also available on OpenAPI 4 device.

Many older devices can have their firmware upgraded to support newer OpenAPI versions. Please contact Konica Minolta to inquire about firmware upgrade availability for your model.

PaperCut makes all attempts to keep the product compatibility information in this manual current. However, we make no warranties, express or implied, with respect to manufacturer's products or the interoperation with the listed PaperCut product(s). We offer 40 day trial versions of PaperCut software to assist you with compatibility testing with your network setup.

4.2 Requirements

Before installing the PaperCut Embedded Application on to the Konica Minolta device, ensure that basic monitoring of network printing has been setup up and tested for this device. The device would show up in the printer list in the PaperCut web interface and have a few print jobs in its print history.

After that, ensure that the following points are checked off before getting started:

- PaperCut is installed and running on your network. Please see the 'Introduction -> Quick Start Guide' section of the PaperCut user manual for assistance.
- Ensure that your Konica Minolta device supports OpenAPI 3.1 or later.
- Ensure that the Konica Minolta device is connected to the network.
- Have available the network name or IP address of the Konica Minolta device.
- It is recommended that the device be configured with a *static IP address*.
- Verify that firewalls or other network restrictions do not prevent the PaperCut server's access to port 50003 on the device and do not prevent the device's access to the PaperCut server on ports 9191 and 9192.
- Ensure the device has a Web browser installed and activated (LK101 upgrade kit). You can check that the "web browser" is listed under 'Administrator Settings > License Settings > List of Enabled functions' on the device.

4.3 Setup Procedure

4.3.1 Configure OpenAPI Settings

1. Log on as administrator on the device's web interface (called "Page Scope Web Connection") under `http://<ip-address-of-device>/`. Tip: The default administrator's password usually is "12345678", on some newer devices it is "1234567812345678".
2. In the "Security" section display the "PKI Settings" subsection. If there is no "PKI Settings" subsection, please ignore this section and refer to Appendix A instead for configuration of older devices.
3. Create a new certificate following these steps. (Even if a certificate is already shown in the "Device Certificate List", this certificate may not be usable for SSL. Please delete it and re-create a new one.)
 - a. Click "New Registration", select "Create and register a self-signed Certificate" and click "OK".
 - b. Fill in the fields with some values about your organization. The values have no functional significance.
 - c. For the "Validity Period", the maximum number of days offered is recommended (usually 3650 = 10 years).
 - d. "Encryption Strength" can be left to the default values.
 - e. Click "OK". The certificate will be generated. You will be asked to switch the device off and on again.
4. Log into the device web interface as administrator again. In the "Security" section display the "PKI Settings" subsection and from the menu on the left, choose "SSL Setting". Change "Mode using SSL/TLS" to "Admin Mode" or "Admin Mode and User Mode" (on some machines: just "enable"). Your web browser will re-login to the web server under "https" mode. You may have to confirm an "invalid certificate" in your browser.
5. Optional: If you are still using the default password, please change it in the "Security" section. Display the subsection "Administrator Password Settings", tick "Password is changed" and enter a new password and click "OK". Keep a record of the password in a safe place, as per normal system management best practice.
6. In the "Network" section, display the subsection "TCP Socket Setting". Tick "Use SSL/TLS" and click "OK". You will be asked to switch the device off and on again.
7. Log back into the administrator web interface, and in the "Network" section display the "OpenAPI" subsection.
 - a. From the "Use SSL/TLS" drop-down list select "SSL Only".
 - b. Make sure the "Port No. (SSL)" is set to 50003.
 - c. All "Certificate Verification Level Settings" should be set to "Do not request" (1st item) or "Do Not Confirm" (all other items), including "Validity Period" which often is set to "Confirm" by default.
 - d. Click "OK".
8. Some newer devices include an OpenAPI password that needs to be removed. To do so, access the administrator settings on the device's panel, not the web interface:
 - a. Press the "Utility" button on the button panel.
 - b. Press "Administrator Settings" on the screen.
 - c. Log in with the administrator password.
 - d. Selection "System Connection" > "OpenAPI Settings" > "Authentication".

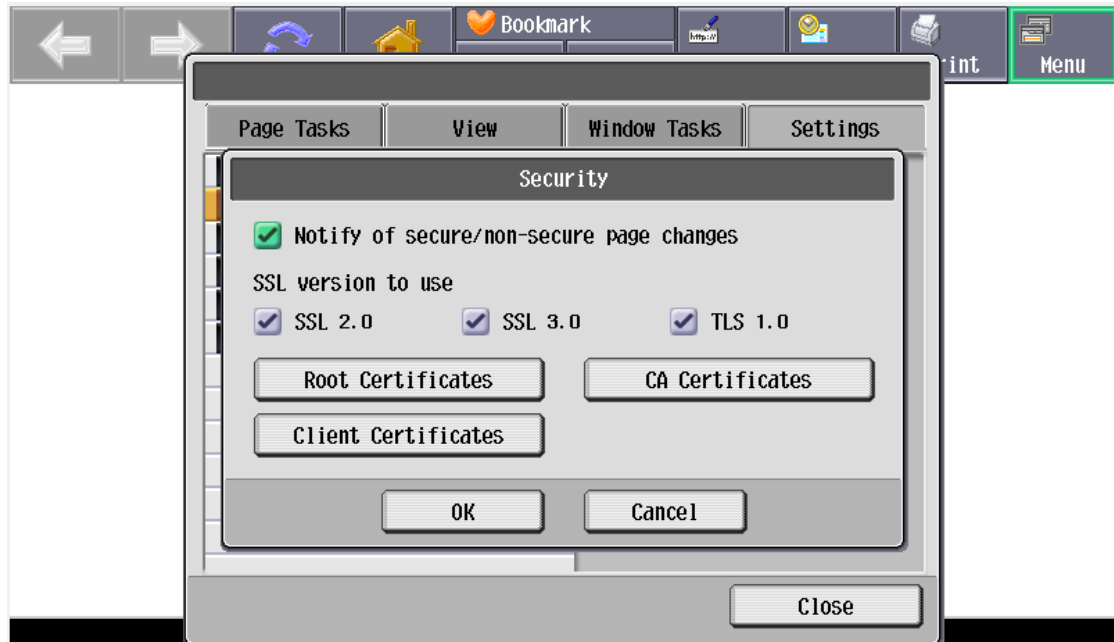
- e. Make sure "OFF" is selected and press "OK".
 9. For security reasons it is also recommended to change the device's default administrator web access password.
 10. Ensure SSDP protocol is enabled under Utility > Administrator > Settings > Network Settings > SSDP Settings.
 11. Ensure WebDAV server is enabled on the device (under Administrator Settings > WebDAV Settings > WebDAV Server Setting). Port 80 on the device will need to be accessible from the PaperCut application server in order to push out application resources over WebDAV.
 12. When MFD is configured for access check you can access the following URL: <http://<MFP IP>/OpenAPI/DeviceDescription/> from the same network location where PaperCut server is deployed, where HOSTNAME is the hostname or IP address of the MFD. If accessed with your web browser the operation should complete successfully and an XML document published by the MFD be displayed.
 13. Check that the web browser is activated on the device prior to proceeding further.
- For example:



If "Web Browser" is not listed, you will need to contact your Konica Minolta dealer and obtain the LK101 upgrade kit and install the browser license on each of your devices (via Install License function in the License Settings).

4.3.2 Web Browser Configuration

Ensure web browser on the device has SSL/TLS connections and JavaScript enabled (under web browser settings).



This requires manually starting the browser application to confirm the settings are okay.

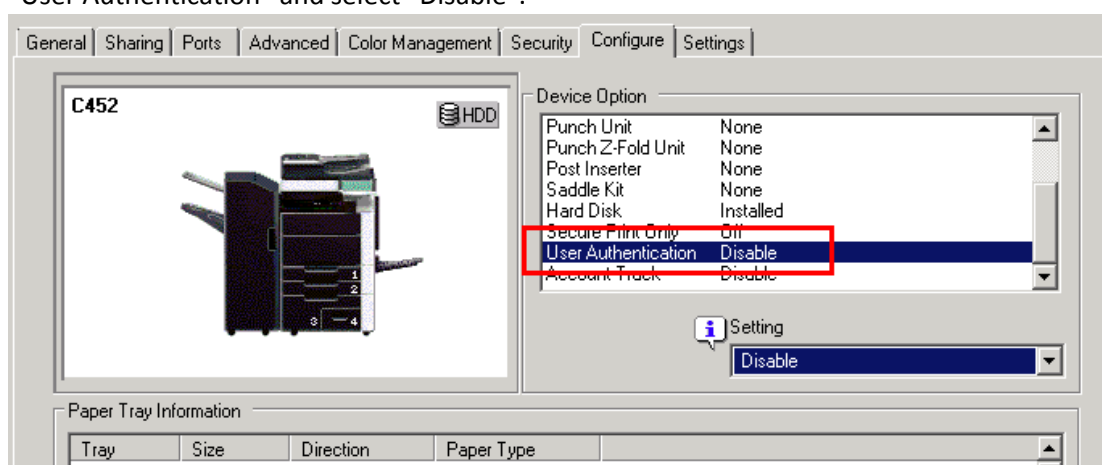
The location of the settings may differ slightly on different models where WebKit browser is used.

4.3.3 Enabling Unauthenticated Printing

When PaperCut is monitoring print queues, it has control of what print jobs are allowed to print. If PaperCut allows a job to print, we do not want the Konica Minolta device to deny the print job or track printing twice (duplicate charging). This requires that print authentication is disabled in the printer driver and on the device, as described below.

Set up a print queue for the Konica MFD on the print server using Konica's print drivers. The driver has to be configured to allow unauthenticated printing. For Windows, right-click the corresponding printer icon in the Printers section of Windows Control Panel and select "Properties". Select the "Configure" tab and:

- Click "Acquire Settings". Make sure the "Auto" check box is **not** selected. Click "OK".
 - NOTE: On some newer models, the "Auto" check box can only be unchecked and saved if the IP address and device administrator password are entered, because the setting is saved on the device.
- At the top right of the "Configure" tab, in the "Device Option" list, scroll down to "User Authentication" and select "Disable".



- Close the Properties window by clicking "OK".

For other operating systems, please consult your Konica documentation.

NOTE: If you are using a virtual queue for load balancing/"find me" printing, then apply the same setting to the virtual queue as well.

In addition, a corresponding device option has to be set on the device, either on the device screen or in the device web interface. Some devices may not offer the option to configure at the device or in the web interface. For configuration at the device screen:

- Press the "Utility/Counter" button.
- Select "Administrator Settings". Enter your administrator password and press "OK".
- Select "User Authentication/Account Track".
- Select "Print without Authentication".
- Select "Allow".
- Select "OK".

For configuration via the web interface:

- Open the device's IP address or hostname in a web browser.
- Log in as the Administrator.
- Select Security -> Authentication -> General Settings.
- Set "Public Access" to "Restrict".
- Set "Print without Authentication" to "Allow".
- Select "Apply".

Alternatively on some copiers it's found via:

- Open the device's IP address or hostname in a web browser.
- Log in as the Administrator.
- Select User/Auth/Account Track.
- Select Print without Authentication
- Set "Print without Authentication" to "Full Color/Black"

The screenshot shows the 'Print without Authentication' settings page. The 'Print without Authentication' dropdown is set to 'Full Color/Black'. The 'IP Filtering (Permit Access)' dropdown is set to 'Disable'. Below these are five IP address ranges, each with a text input field for the IP address and a range selector. The 'OK' and 'Cancel' buttons are at the bottom right.

4.3.4 Additional Device Hardware Settings

If PaperCut fails to operate on some devices, a Konica Minolta certified technician may need to adjust dip switch 25 to "10".

Error message 3, "AuthenticationFunction" in the device status field of PaperCut is often an indication of this setting needing adjusting.

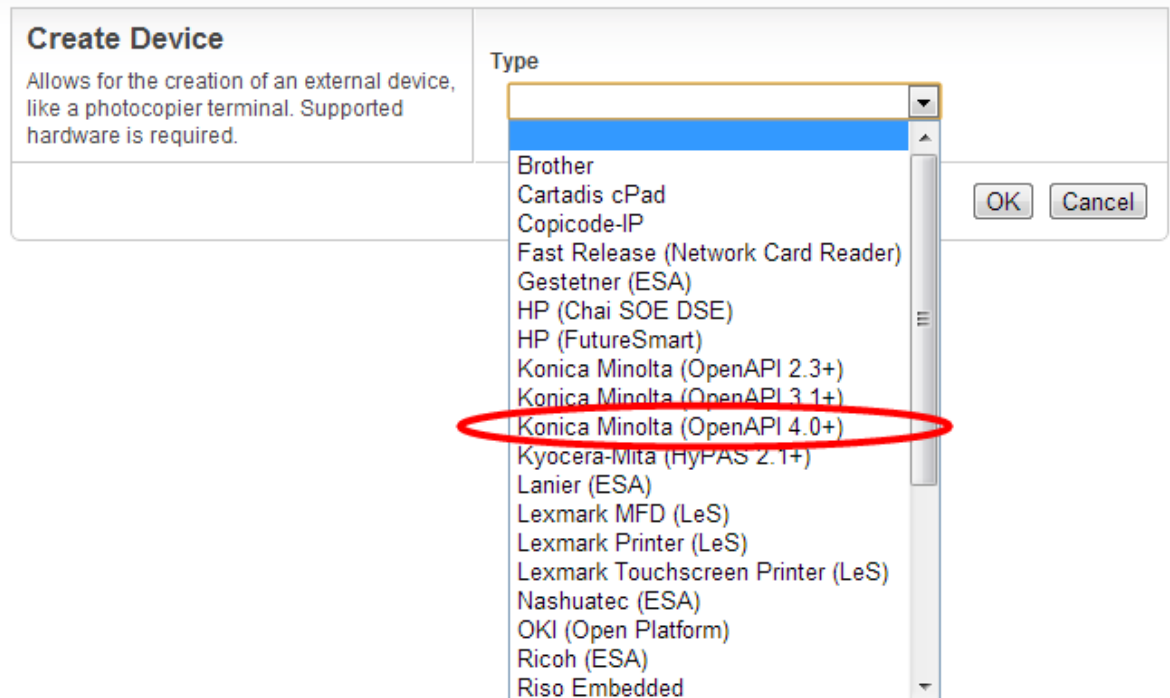
4.3.5 PaperCut Settings

1. **Ensure you are logged out of the device's web interface from the previous step.** PaperCut cannot communicate with the device while an administrator is logged in to the device's web interface.
2. Log in to the PaperCut administration interface using a web browser (e.g. <http://papercut-server:9191/admin>).
3. Navigate to "Options -> Advanced" and ensure the option "Enable external hardware integration" is enabled.

The screenshot shows the 'External Hardware Integration' settings page. The checkbox 'Enable external hardware integration (for supported devices only)' is checked and circled in red.

4. Press "Apply".

5. Navigate to the “Devices” tab.
6. Click “Create Device”.
7. Enter a descriptive name for the device under “Device name”.
8. Enter the device’s network name or IP address under “Hostname/IP”.
9. Optionally enter location/department information.
10. From the “Type” drop down, select “Konica Minolta (OpenAPI 4.0+)” or “Konica Minolta (OpenAPI 3.1+)” depending on the version of OpenAPI supported by your device.



Create Device

Allows for the creation of an external device, like a photocopier terminal. Supported hardware is required.

Type

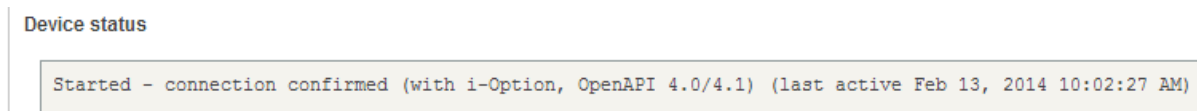
- Brother
- Cartadis cPad
- Copicode-IP
- Fast Release (Network Card Reader)
- Gestetner (ESA)
- HP (Chai SOE DSE)
- HP (FutureSmart)
- Konica Minolta (OpenAPI 2.3+)
- Konica Minolta (OpenAPI 3.1+)
- Konica Minolta (OpenAPI 4.0+)**
- Kyocera-Mita (HyPAS 2.1+)
- Lanier (ESA)
- Lexmark MFD (LeS)
- Lexmark Printer (LeS)
- Lexmark Touchscreen Printer (LeS)
- Nashuatec (ESA)
- OKI (Open Platform)
- Ricoh (ESA)
- Riso Embedded

OK Cancel

11. Enter "Admin" as the administrator username and enter the password set in step 4.3.1.
12. Under “Function”, tick “Track & control copying” and “Enable print release”. Enabling both copy and print release functionality allows for post-installation testing. Chapter 4 shows how to change this setting later.
13. Click “OK”.

4.3.6 Verify Device Creation

The “Device Details” screen will now display, and it has an area titled “Device status” which after clicking the “Refresh” link should show **“Started – setting up device integration...”**. Please click “Refresh” again a few times until the status field shows **“Started - connection confirmed”**:



Device status

Started - connection confirmed (with i-Option, OpenAPI 4.0/4.1) (last active Feb 13, 2014 10:02:27 AM)

While the setup is running, the screen on the device should first go blank with a message “Now remote operating” and after about 30 seconds should show the PaperCut “Authentication” screen with username and password field.

Before proceeding with testing ensure the device has started successfully and no warnings or errors are shown on the device page.

Ensure the screen of the device is displaying the correct interface, for i-Option the display should look similar to this:

Example of the web browser based UI when using i-Option

If i-Option is not active, the UI should appear similar to:

*Example of the Standard Konica Minolta UI when **not** using i-Option*

If everything looks okay, you should now proceed to configure page costs and other settings relating to the device.

4.3.7 Additional Network Security (optional)

The MFP communicates with the PaperCut server over the network (e.g. to authenticate users or release print jobs). To provide an additional level of security, PaperCut may be configured to only allow device connections from a restricted range of network addresses. This ensures that only approved devices are connected to the PaperCut server.

By default PaperCut will allow device connections from any network address. To restrict this to a subset of IP addresses or subnets:

1. Logon to the PaperCut administration web interface at `http://<papercut-server>:9191/admin`
2. Go to the Options→Advanced tab and find the “Security” section.
3. In the “Allowed device IP addresses” field enter a comma-separated list of device IP addresses or subnets (in the format `<ip-address>/<subnet-mask>`).
4. Press the “Apply” button.
5. Test the devices to ensure they can continue to contact the PaperCut server.

4.4 Upgrading to a newer version

The PaperCut Konica Minolta Embedded will be up to date when you upgrade your PaperCut installation; no further action is necessary.

When upgrading from a standard UI version of the embedded software (OpenAPI 3.1) for the first time, the web based interface will not be enabled by default unless a new device is created.

To enable this for an existing device set `ext-device.konica-minolta.browser.enabled` to “Y” under the advanced configuration tab of the device details screen. See section 7.1.

To force all i-Option capable Konica devices to use the standard UI set `ext-device.konica-minolta.browser.enabled` to “N”. See section 7.1.

Generally the configuration settings such as whether the browser is to be enabled will not be touched after upgrade so once it’s set one way or another it will be retained unless explicitly changed by the administrator in PaperCut.

5 Post-install testing

After completing installation and basic configuration, it is recommended to perform some testing of the common usage scenarios. This is important for two reasons:

1. To ensure that the embedded application is working as expected.
2. To familiarize yourself with the features and functionality of PaperCut and the embedded application.

This section outlines four test scenarios that are applicable for most organizations. Please complete all the test scenarios relevant for your site.

The following test cases assume a device with OpenAPI 3.1 or later.

5.1 Test Preparation

To complete these tests it is recommended you use two test users so that each can be configured differently. These users are:

- ‘testusersimple’ – used to perform basic copier monitoring and control and to perform print release tests.
- ‘testuseradvanced’ – used to perform copier monitoring and control with account selection enabled (i.e. to charge copying to accounts/departments/cost-centers/etc).

To setup these users in PaperCut:

1. Create the ‘testusersimple’ and ‘testuseradvanced’ users in your Active Directory or LDAP directory.
2. Login to the PaperCut’s admin web interface
3. Go to the “Options->User/Group sync” page and press “Synchronize Now”.
4. Once the sync is complete, the users will be added to PaperCut.

The next step is to configure the users. To configure ‘testusersimple’:

1. In PaperCut, select the “Users” tab
2. Select the ‘testusersimple’ user.
3. Set the user’s balance to \$5.00 and verify the account is set to “Restricted”.

Account Details
To set the user's balance enter the value here. To adjust the amount (like adding 5 credits), select the 'adjust' link. Making the user 'restricted' means that they will not be able to print when their account has no credit.

Balance
\$5.00 (adjust)

☒ Restricted

Overdraft
Use default overdraft (\$0.00) ▼

4. Verify that this user is set to “Automatically charge to personal account” in the “Account selection” options.

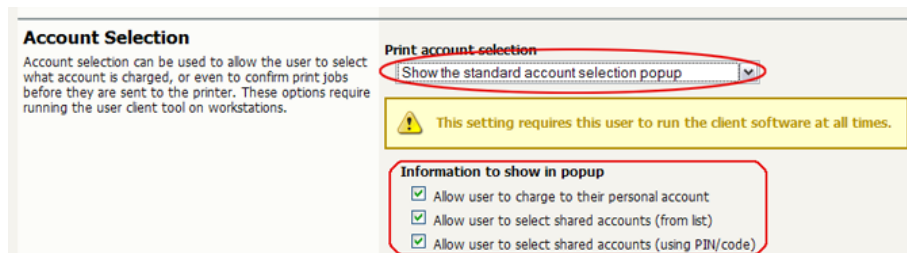
Account Selection
Account selection can be used to allow the user to select what account is charged, or even to confirm print jobs before they are sent to the printer. These options require running the user client tool on workstations.

Print account selection
Automatically charge to personal account

5. Press the “OK” button to save.

To configure ‘testuseradvanced’:

1. In PaperCut, select the “Users” tab
2. Select the ‘testuseradvanced’ user.
3. Change the “Account Selection” option to “Standard account selection popup” and enable all the account selection options.



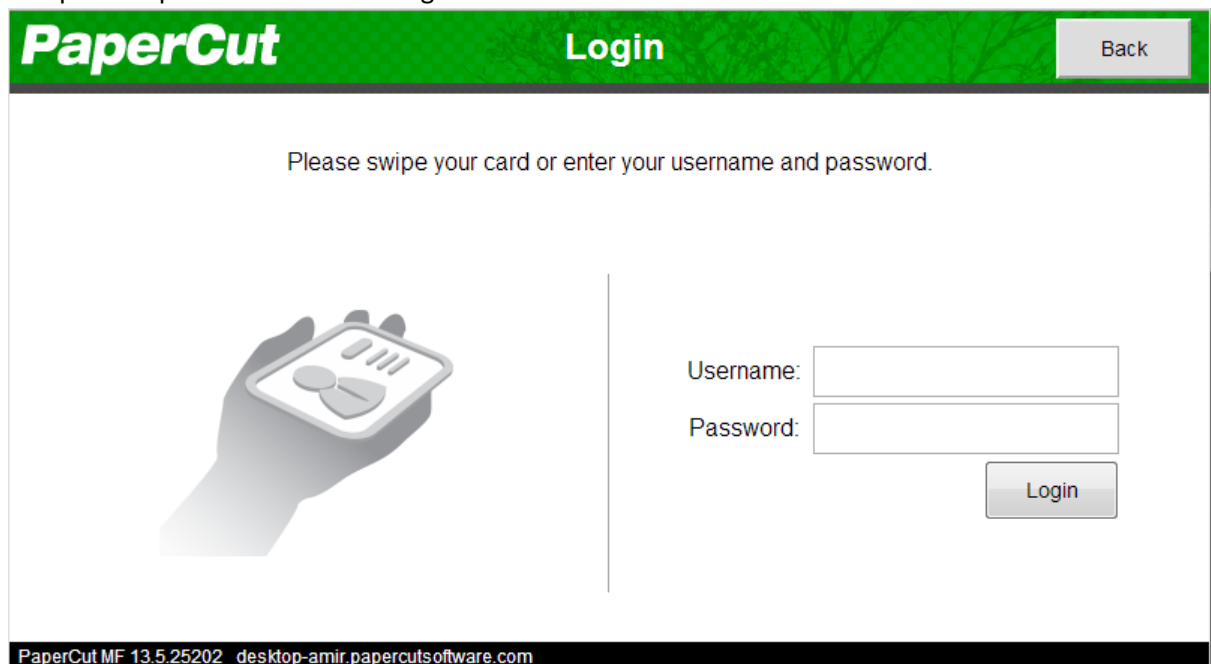
4. Press the “OK” button to save.

5.2 Scenario 1: Standard copying

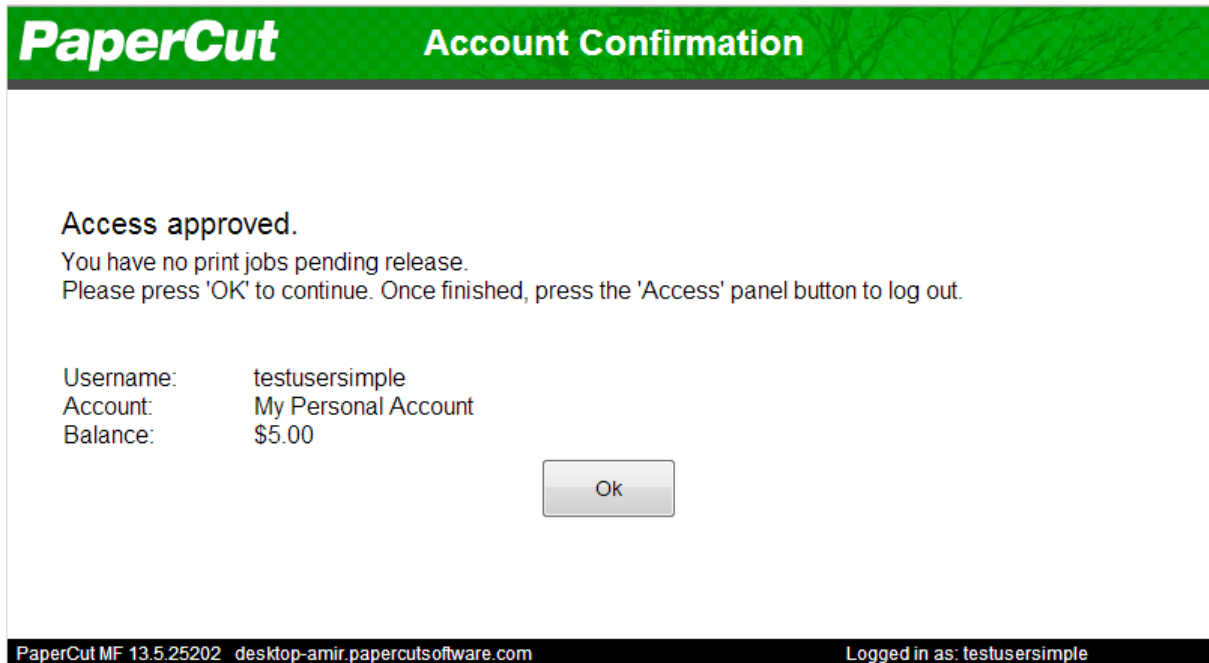
Standard copying involves monitoring and charging printing to a user’s personal account. This is most commonly used for student printing or basic staff monitoring. Users can also be configured for unrestricted printing, which is commonly used for staff/employee use.

At the photocopier:

1. The photocopier should be showing the “Authentication” screen as shown below.



2. Focus on the “Username” field and enter the username “testusersimple” using the on-screen keyboard and press “OK”. Likewise, press the “Password” field and enter the password previously chosen.
3. Press “Login”.
4. The screen will now show a login confirmation:



PaperCut Account Confirmation

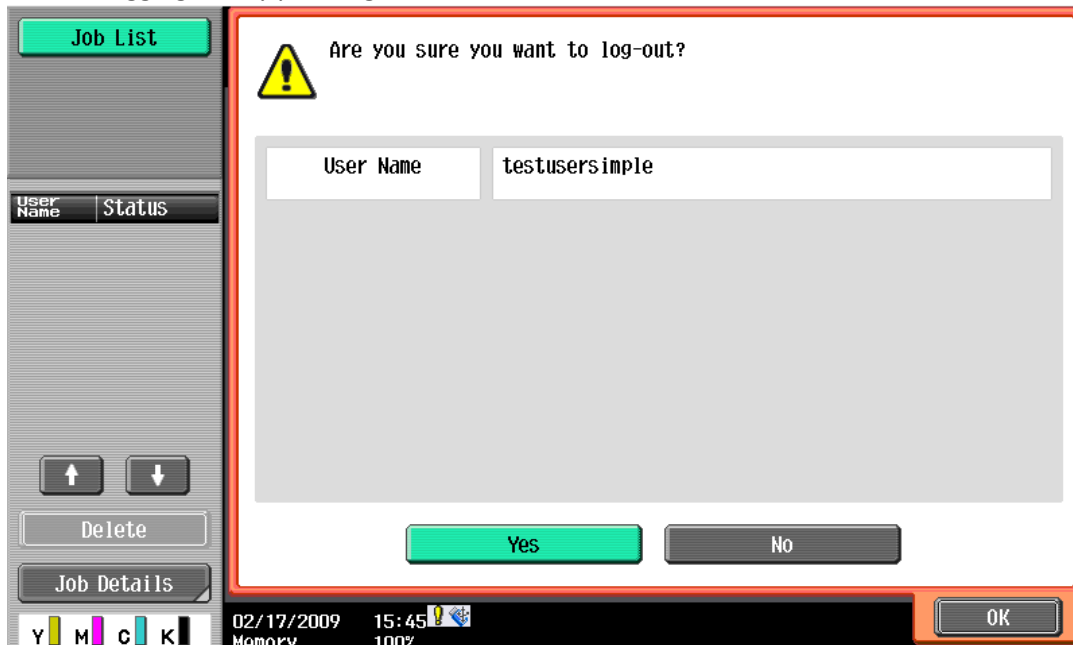
Access approved.
You have no print jobs pending release.
Please press 'OK' to continue. Once finished, press the 'Access' panel button to log out.

Username: testusersimple
Account: My Personal Account
Balance: \$5.00

Ok

PaperCut MF 13.5.25202 desktop-amir.papercutsoftware.com Logged in as: testusersimple

5. At this point the copier will be enabled for usage.
6. Follow the onscreen instructions and perform some test copying, i.e. press the “Start” button on the device button panel and perform a copy as normal.
7. Once completed copying, press the “Access” button on the device’s button panel and confirm logging out by pressing “Yes” and “OK” on the screen.



Job List

User Name Status

Are you sure you want to log-out?

User Name testusersimple

Yes No

Job Details

Y M C K 02/17/2009 15:45 Memory 100%

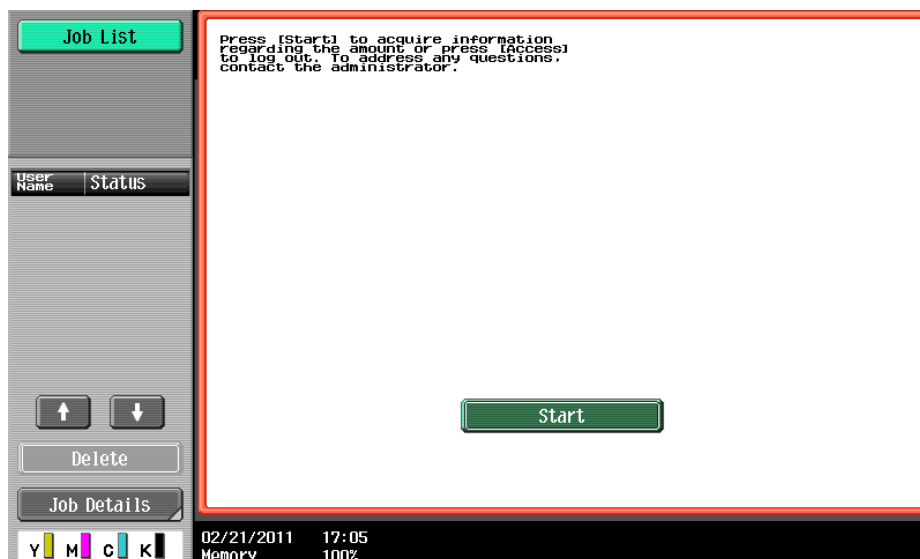
OK

Back in the PaperCut application verify that the copier activity was recorded and the user's account deducted:

1. Log in to PaperCut.
2. Select the device from the "Devices" tab.
3. Select the "Job Log" tab. This will list all recent copying activity on the copier. The copying just performed as the test user should be listed. Verify the details of the copy job that was just performed.

Usage Date ▼	User	Charged To	Pages	Cost	Document Name	Attribs.
Apr 16, 2008 2:59:30 PM	testusersimple	testusersimple	2 (Color: 0)	\$0.20	[copying]	A4 (ISO_A4) Duplex: No Grayscale: Yes

NOTE: If the user runs out of credit while copying, the following warning will be displayed:



At this point the user can only log out by pressing the "Access" button on the copier panel.

5.3 Scenario 2: Copying with account selection

Firstly a test account should be created:

1. Log into PaperCut and select the "Accounts" tab.
2. Select the "Create a new account..." action link on the left.
3. Enter an account name "Test Account 1".
4. Enter PIN/Code "2233".
5. Select the "Security" tab and allow all users to access that account by adding the "[All Users]" group.
6. Press "OK".

At the photocopier:

1. The photocopier should be showing the “Authentication” screen as before.
2. Enter the username (‘testuseradvanced’) and password as before and press “Login”.
3. An account selection screen appears with two account fields. An account is selected by pressing the relevant field.
4. Select “Test Account 1” by pressing the button.

5. The account will be selected and the login will proceed to the next screen.
6. The confirmation screen will show that “Test Account 1” has been selected. Acknowledge by pressing “OK”.

7. Now perform copying as normal, and finally log out using the “Access” button as before.

Back in the PaperCut application verify that the copier activity was recorded and the user's account deducted:

1. Log in to PaperCut
2. Select the device from the "Devices" tab
3. Select the "Job Log" tab. This will list all recent copying activity on the copier. The copying just performed as the test user should be listed.
4. Verify the details of the job (i.e. that the job was charged to the selected account).
5. In the log details, click on the "Charged To" account name to view the account's details.
6. Selecting the "Job Log" tab will display all print/copy activity for the account, and will show the test photocopying that was performed.

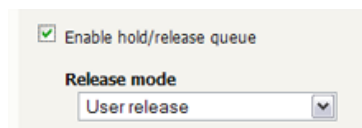
5.4 Scenario 3: Print release

The embedded application may also be used for print release. For a full description of PaperCut hold/release queues and print release, please read the PaperCut manual.

Skip this scenario if hold/release queues will not be used at your site.

To perform print release testing, a hold/release queue must be enabled:

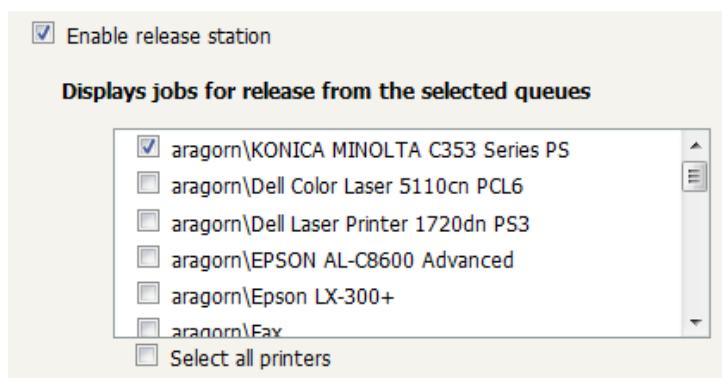
1. In PaperCut, select the "Printers" tab.
2. Select the print queue (i.e. not the 'device') for the Konica Minolta device that will be used for testing.
3. Enable the "Hold/release queue" option.



4. Press "OK" or "Apply" to save the changes. All printing to this queue will now be held until released by a user.

Make sure the copier is enabled as a "Print Print release":

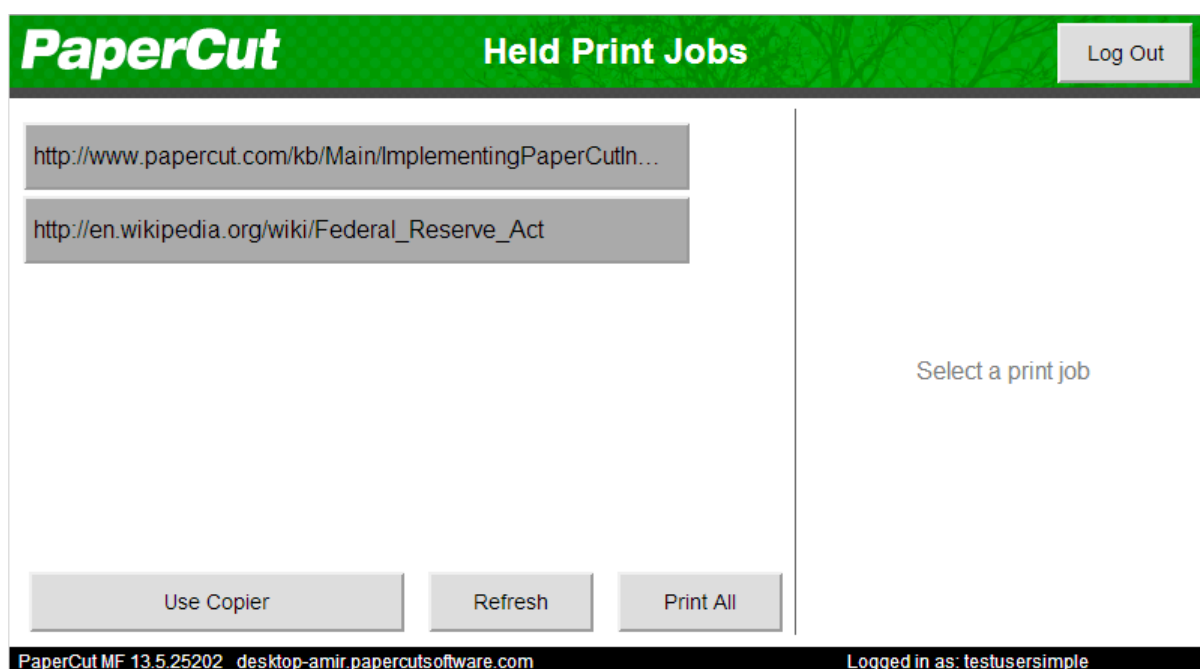
1. In PaperCut, select the "Devices" tab.
2. Select the Konica Minolta device.
3. Under "Device function", make sure "Enable print release" is ticked. If you have followed the installation steps from the previous chapter, this function will already be enabled.
4. Select the print queue that was enabled for hold/release above. The Konica Minolta device will allow jobs on the selected queues to be released.



5. Press "OK" to save.
6. Login to a computer workstation as 'testusersimple'.
7. Print a few jobs to the print queue that was configured above. The jobs will be held in the hold/release queue.
8. Confirm that the jobs are held, by checking that the jobs are listed in the "Printers -> Jobs Pending Release" page of the PaperCut administration interface.
9. Confirm that the username is 'testusersimple'.

At the device:

5. Log in with the 'testusersimple' username and corresponding password, as in scenario 1.
6. The web browser based interface allows for print release to be done immediately after authenticating, without unlocking the device. Any held jobs will be shown in the print release screen:



7. A list of print jobs will show. You can highlight and deselect individual items by pressing the list item:

PaperCut Held Print Jobs Log Out

<http://www.papercut.com/kb/Main/ImplementingPaperCutIn...>

http://en.wikipedia.org/wiki/Federal_Reserve_Act

Document: <http://www.papercut.com/kb/Main/ImplementingPaperCutInSchools>

Printed By: testusersimple

Time: 8:34 AM

Client: DESKTOP-AMIR

Pages: 3

Cost: \$0.03

Use Copier Refresh Print All Print Delete

PaperCut MF 13.5.25202 desktop-amir.papercutsoftware.com Logged in as: testusersimple

8. Selecting a job will show the details of the job next to the job list item.
9. Note that jobs can be released without unlocking the device. To use the device, press the "Use Copier" button to continue the login workflow.
10. Once logged in, print release can be accessed via the release button.

Ready to copy. Copies: 1

No Animation Guide data available.
Contact your administrator.

Job List Check Job Release Check Details

Basic Original Setting Quality/Density Application

Color Auto Color

Paper Auto Paper Select

Zoom 100.0%

Duplex/Combine 1 to 1

Corner Staple Top Left Finishing Separate Scan Auto Rotate OFF

Y M C K 05/22/2012 18:46 Memory 100% Language Selection

11. Jobs can be printed using the "Print" button on individual jobs or "Print all" where available, to print all the jobs at once.
12. Cancelling jobs is done using the "Delete" button.
13. Similarly, the "Use Copier" button returns to the copier interface.
14. To log out, press the "Access" button on the device's button panel and confirm by pressing "Yes" and "OK".

5.5 Scenario 4: Scanning and faxing

Konica Minolta devices can also scan documents and send them by email. If a phone line is attached, they can also send faxes. You can enable the tracking of scanning and faxing, and prevent users from scanning or faxing when they are out of credit.

To enable tracking of scans and faxes:

1. In PaperCut, select the “Devices” tab.
2. Select the MFD name.
3. Under “Device function” tick “Track & control scanning” and “Track & control faxing”.
4. Select the charging type “advanced” in both cases, and set some numbers for page costs and thresholds. The cost after the threshold should be lower than the standard cost, as it represents a volume discount. As an example, the screen shot below shows that the first page of a fax is charged at \$0.20 and any subsequent page at \$0.10.

At the photocopier:

1. Log in using username and password as ‘testusersimple’.
2. The copier will initially show the copy settings screen. Press the “Fax/Scan” button on the device panel to do some scanning, and send some faxes.
3. Once completed scanning and faxing, log out by pressing the “Access” button on the device panel and confirm “Yes” on the screen.

In the PaperCut administration interface, verify that the scan and fax activities were recorded and the user’s account was deducted. This can be done as follows:

4. Log in to the PaperCut administration interface.
5. Select the device from the “Devices” tab.
6. Select the “Job Log” tab. This will list all recent activity on the copier, including copying, scanning and faxing. The jobs just performed as the test user should be listed. Verify the details of the jobs that were just performed.

Usage Date ▼	User	Charged To	Pages	Cost	Document Name	Attrib
Dec 9, 2009 11:45:23 AM	testusersimple	testusersimple	2	\$0.30	[fax]	
Dec 9, 2009 11:44:35 AM	testusersimple	testusersimple	5	\$0.30	[scanning]	

7. Click on the user's name in the user column to view the user's account details.
8. Select the "Job Log" tab to display all activity for the user.
9. Select the "Transaction History" tab and verify that the cost of the scans and faxes was deducted from the user's account.

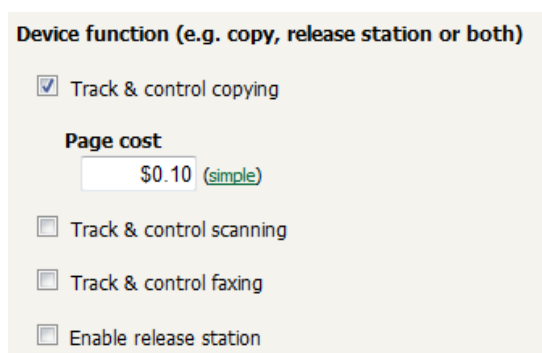
<u>Transaction date</u> ▼	<u>Transacted by</u>	<u>Amount</u>	<u>Balance after</u>
Dec 9, 2009 11:45:23 AM	[system]	-\$0.30	\$4.40
Dec 9, 2009 11:44:35 AM	[system]	-\$0.30	\$4.70

6 Configuration

After completing the Installation section and registering the device with PaperCut, it will have been configured with reasonable default settings that are suitable for most environments. This section covers how to change the default settings. All of the following settings are available via the device's "Summary" tab in the PaperCut administration interface.

6.1 Device Function

The device function setting defines which functions will be available on the device and how it will be used. Not all function settings are supported on all devices.



Device function (e.g. copy, release station or both)

☒ Track & control copying

Page cost
\$0.10 [\(simple\)](#)

☐ Track & control scanning

☐ Track & control faxing

☐ Enable release station

Each device function is discussed in the following table.

Device Function	Description
Track & control copying	The device will track walk-up off-the-glass copying.
Track & control scanning	The device will track scanning such as scan-to-email or scan-to-file.
Track & control faxing	The device will track the sending of faxes.
Enable print release	The device will act as a print release station.

6.2 Authentication Methods

PaperCut supports a number of different ways to authenticate users who walk-up to the devices to perform copying. The default authentication method is username and password authentication.

The available authentication methods can be modified in the 'External Device Settings -> Authentication methods' section.

Authentication methods

- ☒ Username and password
- ☒ Identity number
 - ☐ Require PIN
- ☐ Swipe card
- ☐ Automatically login as user

Authentication methods available for a device

Not all authentication methods are supported on all devices. A grayed-out option indicates that the option is not supported on this device.

Each authentication method is discussed in the following table.

Authentication Method	Description
Username and password	The user may use their domain/network username and password to log into the device.
Identity number	The user may log in with their identity number. Identity numbers are convenient when usernames are long or cumbersome to enter. For example, rather than entering a username like 'john.smith.001', it may be more convenient to enter an employee ID of '1234'. See the PaperCut user manual for information about user identity numbers, including importing identity numbers from an external source.
Identity number -> Require PIN	When a user logs in with their identity number, they must also provide their associated PIN. This provides additional security for identity number logins.
Swipe card	The user may log in by swiping a card (e.g. smart card, RFID card or any other card supported by the device). See the PaperCut user manual for information about user card numbers, including importing card numbers from an external source.
Swipe card -> Require PIN	When a user logs in by swiping a card, they must also provide their associated PIN. This provides additional security for swipe card logins.
Automatically login as	Specifies that this device should always automatically log in as the given

user	user. This option overrides all other authentication methods
------	--

Description of authentication methods

6.3 Customizing Text and Messages

PaperCut allows some text that appears in the device to be customized. The custom text might include instructions or terminology that is more appropriate for the installation site. An example of text that is customizable is the “welcome text” that displays before the user logs in to the device.

The text can be customized by editing the device configuration from the PaperCut administration interface. For more details, see the Advanced Configuration section.

7 Advanced Configuration

7.1 Config Editor

The common configuration options for a device in PaperCut are available on the device's "Summary" tab, and are discussed in more detail in the Configuration section. This section covers the more advanced or less common configuration options which are available via the "Advanced Config" tab in the device details screen.

Config name	Description
ext-device.card-self-association.use-secondary-card-number	<p>Select whether user self-association should occupy the primary or secondary card number. It overrides the global setting unless the keyword "GLOBAL" is specified. This is useful when there is a mix of different non-configurable card readers that read different numbers from an ID card.</p> <p>Set to "Y" to use the secondary card number, "N" to use the primary card number. Default: "GLOBAL" to defer to the global configuration option.</p>
ext-device.konica-minolta.login.show-account-search	<p>If set to "Y" replaces the "Account List" button next to the "Account" for account selection field shown during logon to users with account selection enabled with a "Search" button. "Search" allows searching accounts by text, pressing "OK" at search text entry will display all accounts.</p> <p>This is convenient for users with many potential accounts to charge to. However, this will be enabled for all users including those with short account lists, who will need to press "OK" at search text entry to display the whole list.</p>
ext-device.konica-minolta.locale	<p>Enter the locale (language setting) for display on the device in the form "xx" or "xx_XX" if different from the server. Examples: "fr" or "pt_PT".</p>

ext-device.konica-minolta.message.welcome.line1 and ext-device.konica-minolta.message.welcome.line2	Specify two lines of text to appear on top of the “Authentication” screen in place of the default message. These can include instructions on which username and password are valid for the device. The value “DEFAULT” in both fields will re-enable the default text.
ext-device.konica-minolta.auth.screen.title	Change the title of the authentication screen.
ext-device.konica-minolta.login.host-based.enabled	<p>Enables support for external host-based authentication (eg TWAIN based scanning, PageScope Web Connection) if set to “Y”.</p> <p>Otherwise external authentication is not allowed (other than logging-on physically on the MFP).</p> <p>Users are required to login using username and password.</p> <p>See section 7.5.</p>
ext-device.konica-minolta.login.host-based-authentication.enabled	<p>Enables secured login for external host-based authentication (if host-based logins are enabled).</p> <p>If set to Y,</p> <p>Users connecting via “PageScope Web Connection”, TWAIN or another external mechanism will need to provide valid credentials.</p> <p>Concurrent use of device externally while someone else is logged on physically is disallowed.</p> <p>Note that on some models enabling this option may interfere with USB printing reliability.</p> <p>If set to N,</p> <p>Users are not required to provide valid credentials to perform TWAIN scanning or login to the device externally.</p> <p>See section 7.5.</p> <p>Default: N</p>

`ext-device.konica-minolta.appno.auth` and `ext-device.konica-minolta.appno.pullprint`

Some Konica Minolta devices may have other embedded applications installed such as “Pull Print” applications that allow easy access to print documents from a repository of often-printed documents. These applications occupy “application slots” in the device numbered from 1 to 10 or higher and may conflict with PaperCut which by default occupies slots 1 and 2. If either slot is occupied by another application, change the value to a free slot here.

`ext-device.konica-minolta.login.confirmation.enabled`

Setting this to “N” allows you to bypass the confirmation screen shown after a successful login.

Note that this was replaced in by the standard configuration checkbox “Show account confirmation” on the device summary tab. The old setting will be automatically migrated across.

Device Options

☒ Show account confirmation

Device status

Started - connection confirmed (last active Jan 16, 2014 8:38:28 AM)

`ext-device.card-no-regex`

See chapter 7.3 “Configuring Swipe Card Readers”

`ext-device.konica-minolta.restricted.allow-multiple-login`

Setting this to “Y” will allow users to log in and charge copy jobs to a restricted account (user account or shared account) if another copy job charged to the same account is still in progress. This may cause cost overruns with users going into negative balance.

`ext-device.konica-minolta.card-decoder-hid`

Selects the method used to read a user ID from an HID RFID card reader. 0 → the card number field from OmniKey readers is used as the PaperCut user ID. 1 → the entire data on the reader is used as the PaperCut user ID.

ext-device.konica-minolta.card-decoder-force-mode	<p>Overrides card reader auto detection and forces a decode mode, useful where reader detection and consequently decoding of card numbers is unreliable.</p> <p>Currently supports the following values:</p> <p>DEFAULT - Automatic mode</p> <p>AU201 – Force decoding of numbers compatible with AU201 card reader</p> <p>RAW_HEX – Skip decoding and output hexadecimal encoded values sent from the card reader as is, useful for interfacing with custom JavaScript converters.</p>
ext-device.konica-minolta.email.personalized-sender	<p>If set to “Y” will pre-populate the email address in the device’s Scan-to-Me function as stored in the user’s details in PaperCut</p>
ext-device.konica-minolta.display-balance	<p>If set to “Y” will display the balance on the device’s screen while using copier functions. Display will not be accurate for users with overdrafts. Unrestricted users will display as “99999999”. Set to “DEFAULT” or “N” to not display balance.</p>
ext-device.konica-minolta.skip-setup	<p>If set to “Y” will skip reconfiguring the device each time a setting is changed the PaperCut administrator interface or the server is restarted. Must be set back to “N” to apply settings. Use with care.</p>
ext-device.konica-minolta.escrow-timeout.mins	<p>Period of any one user’s inactivity (default: 60 mins) after which the user is assumed to have left the device and finished all copying in case a “log out” has not been reported by the device, e.g. in case of network outages or device firmware defects. The user will then be granted access to his remaining funds in case of escrow and restricted users are allowed to log in again. Please consult with support before changing this option.</p>
ext-device.konica-minolta.late-job-timeout.mins	<p>Period of any one user’s inactivity (default: 5 mins) after which jobs performed following the escrow timeout are logged (see above).</p>

ext-device.konica-minolta.session-timeout.mins	Period of any one user's inactivity (default: 1440 mins = 24 hours) during which jobs started in the user's session can be finished and accounted for in case a "log out" has not been reported by the device due to network outages or device firmware defects. Please consult with support before changing this option.
ext-device.konica-minolta.compatibility-mode	Modifies job logging and accounting behavior to accommodate scanning and other embedded applications that rely on the authenticated user name on the device. Enabling this option invalidates zero-stop handling and shared accounts. <u>Please consult with support before changing this option.</u>
ext-device.konica-minolta.login-confirmation-message	Allows for optional text to be configured and presented on the device, as part of the overall login confirmation screen message and instructions.
ext-device.konica-minolta.app-button.title	<p>Configures an optional custom title for the application button label that appears on the application list screen if print release application is installed.</p> <p>For example instead of using default label of 'Release' for print release application, this can be set to the desired custom value. This affects both the link label displayed on the device and the application name.</p>
ext-device.konica-minolta.app-release.title	<p>Allows customising of the PaperCut's print release application title without also customising the link label that appears on the device screen.</p> <p>If there are multiple applications installed on the device such as a third party application together with PaperCut print release application, they may be grouped together on the device in a separate screen.</p> <p>In this scenario the link button on the device panel may need to be customised to something generic, and PaperCut print release app to something specific, in such case use ext-device.konica-minolta.app-release.title to define the title for PaperCut application, whilst using ext-device.konica-minolta.app-button.title to define the name of the group of applications.</p>

ext-device.konica-minolta.accounts.initial-tab	<p>Set to "LIST", "SEARCH" or "CODE" to make the Account Selection screen start on the "From List", "Search" or "By Code" tab respectively.</p> <p>If you have many shared accounts you may wish to set this to "SEARCH". An example of this is legal firms who use shared accounts for matter codes.</p> <p>Default: "LIST"</p>
ext-device.konica-minolta.login.show-release	<p>Specify whether to include the "Print Release" screen in the login workflow if the device is configured as a release station. Values: Y, N. Default: Y</p> <p>If set to "N", the user must login and press the "Release" button on the device screen to access the release jobs application.</p>
ext-device.konica-minolta.release.show-cost	<p>Specify whether to show the Job cost for each print job. Values: Y, N. Default: Y.</p>
ext-device.konica-minolta.release.list-format	<p>Allows configuring the format of the job listing on the print release screen. This is a customisable format string that can be built up using a combination of well-known tokens such as:</p> <ul style="list-style-type: none"> %document% - job title %user% - job user %pages% - job pages %time% - job time %cost% - job cost %client% - job client <p>Default: %document%</p>
ext-device.konica-minolta.browser.enabled	<p>Allows the browser based interface to be switched on and off. When switched off, the i-Option embedded operates as the standard UI embedded application using the standard Konica Minolta UI.</p> <p>Values: Y, N. Default: Y.</p>

ext-device.konica-minolta.browser.screen-height	<p>Overrides the auto detected panel resolution/screen height. When set to a positive integer, the value represents the screen height in pixels.</p> <p>Default: 0 (auto)</p>
ext-device.konica-minolta.browser.screen-width	<p>Overrides the auto detected panel resolution/screen width. When set to a positive integer, the value represents the screen width in pixels.</p> <p>Default: 0 (auto)</p>
ext-device.konica-minolta.browser.connection-timeout.secs	<p>Specifies any connection timeouts that apply for browser operations in seconds.</p> <p>Default: 30 seconds (1-300 seconds)</p>
ext-device.konica-minolta.browser.header-color	<p>Customizes header color, see section 7.7</p>
ext-device.konica-minolta.browser.show-logout-button	<p>Allows logout button to be hidden in the login interface. Users can logout while in the middle of the login workflow by pressing the “reset” key on the device panel instead.</p> <p>Default: Y</p>
ext-device.konica-minolta.browser.show-back-button	<p>If back button is shown in the login interface it can be hidden similarly to ext-device.konica-minolta.browser.show-logout-button.</p> <p>Default: Y</p>
ext-device.konica-minolta.browser.header-text-color	<p>Customizes header text color, see section 7.7</p>

<p>ext-device.konica-minolta.keyboard-adaptive</p>	<p>Enables PIN and password controls to use adaptive keyboard type. Adaptive keyboard will use a soft keyboard that is most suitable to the MFP location and provides support for locale specific symbols.</p> <p>Y enables adaptive keyboard, N uses ASCII keyboard</p> <p>Values: Y, N. Default: N</p> <p>Note. Supported on models C652/C552/C452-1st onwards, if embedded integration fails on older models, disable this by setting it to N.</p>
--	---

<p>ext-device.konica-minolta.keep-device-settings</p>	<p>Enables some device customizations to be retained after embedded restart and re-installation (on supported models).</p> <p>The customizations include any registered home screen shortcuts and public user function limitations.</p> <p>Values: Y, N. Default N</p>
---	--

<p>system.inactivity-timeout-secs</p>	<p>Sets custom timeout value during login workflow, if the device is unattended for more than the number of seconds defined in this setting the login screen will be aborted and returned to the initial screen. Note that MFP's own reset time-out settings can interfere with this value if set inconsistently.</p> <p>Default: 60 seconds</p>
---------------------------------------	--

Additional options for OpenAPI 4.0 devices

<p>ext-device.konica-minolta.browser.show-status-bar</p>	<p>Allows the web browser to be used completely in full screen mode, by disabling the status-bar. Set to "Y" to show the status bar, "N" to hide it and display the UI in full screen.</p> <p>Values: Y, N. Default: N</p>
--	--

7.2 Setting an explicit PaperCut Server Network Address

The copier connects to the PaperCut server to validate user credentials, display print jobs for release, etc. The device makes inbound network connections to the PaperCut server using a network address of the PaperCut server. By default, PaperCut will use the server's IP address. If the server has multiple IPs (i.e. multi-homed) then PaperCut will select one of them. However, on some networks this address (in both cases) may not be publicly accessible from other parts of the network.

If the PaperCut server has a "public" IP address or DNS name, then this can be used instead, which allows the copiers to use the "public" network address instead of the IP address that PaperCut detects. To do this:

- Login to PaperCut
- Go to the "Options" tab.
- Select "Config Editor (Advanced)", from the action links on the left.
- Find the "system.network-address" setting.
- Enter the public network address for the PaperCut server.
- Press the "Update" button next to the setting and confirm the setting is updated.

When connecting devices to a PaperCut site server, you can configure the sites' "Network address used by devices":

- Login to PaperCut
- Go to the "Sites" tab.
- Select the site to edit.
- Change the "Network address used by devices".
- Save the site details.

To have either of these changes take effect immediately, restart the PaperCut Application Server service (i.e. on Windows use: Control Panel-> Admin Tools-> Services).

7.3 Configuring Swipe Card Readers

At the time of writing, Konica Minolta devices only support the following reader types:

1. AU-201 (MIFARE/Type-A cards).
2. AU-201H / HID Omnikey CardMan 5125 (HID Proximity cards).
3. AU-202H (HID iClass cards)
4. AU-205H / HID Omnikey 5427CK (HID Proximity/MIFARE/Type-A cards).
5. Network card readers (Elatec TWN3 with the TCP Converter/RFIdeas ethernet card readers).
These are set-up similarly to the “Fast Release” configuration in PaperCut where the device is associated with the network reader via its IP/port.

Compatible card readers are limited to those supported by Konica Minolta firmware. PaperCut's embedded solutions are designed to support as many card readers as possible and will add new card reader support at the firmware level, as new devices become available.

The AU-202H readers which are HID proximity card readers will work in place of AU201, but extraction of real card numbers is only possible via a custom JavaScript converter.

Some models do not support all of the listed readers. Please confirm the specifics for the model in question with your local Konica Minolta dealer.

Swipe cards contain numbers used to identify users according to the card number configured in the User Details screen under “Card/Identity” number. Some readers report information in addition to the number encoded on the card, such as checksums. PaperCut can treat these cases in three ways:

Card Number Needs No Conversion

- A typical case is the checksum being reported after the card number, separated by an equals sign, such as 5235092385=8. PaperCut can handle this case by default; it will extract the number before the equal sign as the card number: 5235092385.

Regular Expression Filters

- For some cases, a “regular expression” *may* be required that will filter the card number from the complete string of characters reported by the card reader. Documentation on regular expressions can be found on the Internet, e.g. at www.regular-expressions.info.
 - The regular expression must be fashioned so the card number is returned as the first match group.
 - Usually one regular expression will be used for all the devices managed by PaperCut. This must be entered in “Config editor (advanced)” which is located on the “Options” tab under “Actions”. The key is called “ext-device.card-no-regex”.
 - Additionally, the global setting can be overridden on a per-device basis: The key “ext-device.card-no-regex” can also be found on the “Advanced Config” tab in the device details screen. This setting will override the global setting unless the keyword “GLOBAL” is specified.
 - PaperCut developers will gladly assist in producing a regular expression when supplied with a few sample outputs from your card reader. Please contact PaperCut support.
 - If you would like to write your own regular expressions, here are some examples:

- Use the first 10 characters (any character): `(.{10})`
- Use the first 19 digits: `(\d{19})`
- Extract the digits from between the two “=” characters in “123453=292929=1221”: `\d*=(\d*)=\d*`

Card Number Format Converters

In addition to extracting parts of the card numbers using regular expressions, converting numbers from one format to another is a common requirement. For example a card reader may report in hexadecimal format, while the number stored in the source (e.g. Active Directory) is in a decimal format. PaperCut includes a number of inbuilt converters to assist here.

Note: Many card readers are configurable - the number format can be changed at the hardware level via utility or configuration tools. PaperCut’s software-level converters are there to support card readers that don’t offer this level of configuration, or where a global software-level conversion is a better choice. For example it may be quicker to do the conversion in PaperCut rather than manually reprogram 100+ readers!

Like regex’s, the convertors may be defined on either a global (all devices) or a per-device basis.

To set globally:

- Options -> Actions -> Config Editor
- Search for “ext-device.card-no-converter”
- Enter the name of the required converter (see table below) and click **Update**

To set at the device level:

- Devices -> [select device] -> Advanced Config Editor
- Search for “ext-device.card-no-converter”
- Enter the name of the required converter (see table below) and click **Update**

Standard Converters

Converter	Description
hex2dec	Convert a hexadecimal (base 16) encoded card number to decimal format. Hexadecimal numbers usually contain 0-9 and A-F. This will convert “946EBD28” to “2490285352”.
dec2hex	Convert a decimal encoded card number to hexadecimal format. This will convert “2490285352” to “946EBD28”.
ascii-enc	Unpack an ASCII encoded card number string. E.g. given the number “3934364542443238”, the ASCII code “39” is converted to 9, “34” -

> 4, "45" -> E, with the entire number resulting in "946EBD28".

javascript:<path> Advanced: Define a custom conversion function in JavaScript (see below)

It is possible to chain or pipeline converters by delimiting with a pipe (|). For example, `ascii-enc|hex2dec` will first unpack the encoded ASCII number then convert it to a decimal.

Tip: Not sure which converter to use? Often trial and error is a good approach. After presenting a card, the number will appear in an application logger message with conversions applied (assuming the card is unknown to the system). Try different converters and inspect the resulting numbers in the application log.

Using custom JavaScript

If the inbuilt converter functions are unable to meet requirements, it is possible to define your own function using JavaScript. This is an advanced exercise and it is expected that any implementer be familiar with programming and JavaScript. To implement your own converter:

1. Create a file text file `[app-path]/server/custom/card.js`
2. Define a single JavaScript function in this file called "convert" It should accept and return a single string. Here is a trivial example:

```
function convert(cardNumber) {  
    return cardNumber.substring(3,10).toLowerCase();  
}
```
3. Enter a converter in the form: `javascript:custom/card.js`

Tip: Check the file `[install-path]/server/log/server.log` when testing. Any scripting errors will be displayed as warning messages in the log.

Tip: A Javascript script may also be included in the pipeline. For example

`ascii-enc|hex2dec|javascript:custom/card.js`

Other advanced notes

- If *both* a regular expression and a converter are defined, the regular expression is applied first. This means a regular expression can be used to clean up the input (e.g. remove checksum or delimiters) before passing to a converter.
- In some special situations, a custom JavaScript implementation may not be enough. For example, there may be a requirement to use a 3rd party system to decrypt the number. PaperCut includes an advanced plugin architecture that the PaperCut Software development team uses to implement these advanced converters. Please contact support to discuss development options and costs.

7.4 Card Self-Association

Card self-association allows users to associate their card, or a new card, with this domain account directly at the device.

7.4.1 Self-Association Workflow

The user is notified of the need for self-association and taken to the self- association screen, which is analogous to the login screen.

PaperCut Card Association Back

Enter username and password to associate your card with an existing account.

Username:

Password:

Set

PaperCut MF 13.5.25202 desktop-amir.papercutsoftware.com

The process works as follows:

1. The user swipes a card not known to PaperCut at a device with card self-association enabled.
2. The device gives the user the option to associate the card with their account via a separate self-authentication screen.
3. If the username and password match a valid domain username and password, the card number is remembered and associated with this user thereafter – the user may use this card to access devices without requiring them to enter their username and password.

7.5 Host-based authentication

Host-based authentication refers to any external login to the MFP (originating from another host).

This can be a desktop application such as a TWAIN driver or a web based application such as “PageScope Web connection”.

Desktop based scanning applications using TWAIN drivers to communicate with the device require “host-based authentication” to be enabled.

In this case a device-controlled driver or software pops up a dialog to collect any credentials and to have the user confirm their action.

PaperCut has limited support for applications requiring host-based authentication. This support can be enabled via the advanced configuration option “ext-device.konica-minolta.login.host-based” (see section 7.1).

Applications requesting host-based authentication will cause a popup to display on the desktop showing username/password fields and an input field labeled “account” and “OK” and “Cancel” buttons. The account field is a dummy field, owing to limitations of the device, and any input will be discarded. The user is to use their username and password to authenticate and go ahead with an action, such as scanning.

NOTE: It is possible to allow use of anonymous logins for host-based sessions (see section 7.1).

NOTE: No tracking or charging of jobs requiring host-based authentication will occur by default. Should a user be logged in on the device’s panel at the same time the job is authenticated at the desktop, the job will be charged to the user logged in at the panel.

7.6 Customizing the Header Logo

The embedded application displays a logo in the top left corner of the device screen. This logo can be replaced with your organization’s own logo image.

The image must be saved as a PNG file with the filename “logo.png” and be 42 pixels high.

Save the image on the PaperCut application server at the location:

```
[PaperCut Install Location]\server\custom\web\device\konica\ioption\
```

You will need to create these folders if not present.

The embedded application will fetch the logo image from this location if present. After copying your logo into position, verify it correctly appears in the embedded application.

7.7 Customizing the Header Colors

The header colors are defined in the “Advanced Config” tab in the device details screen, see Config Editor. The options to change are:

- ext-device.konica-minolta.header.color – the background color (type DEFAULT for the default setting of dark green)
- ext-device.konica-minolta.header.textcolor – the text color (type DEFAULT for the default setting of white)

The colors are specified using the hexadecimal web/HTML notation (#RRGGBB) where “RR” is the red component, “GG” is the green component and “BB” is the blue component.

7.8 Customizing the Application Logo Icon

On device models where application logo icons are supported, PaperCut applications installed on the device will have the PaperCut logo set on the application shortcut. Note that the shortcut is only shown where multiple applications are present (including third party) or otherwise if the shortcut to the application is manually created on the main listing screen.

The embedded application will automatically use any icon named icon.png during the setup process, when placed in the following location:

```
[PaperCut Install Location]\server\custom\web\device\konica\ioption\
```

Note, that the icon must be 48x48 pixels and be in the MFD specific variant of the PNG format, which can only be created using Konica Minolta tools/OpenAPI SDK.

8 Uninstalling

In order to remove PaperCut authentication and print release functionality from the device:

- Make sure the device is switched on, connected and the status on the “Device Details” screen shows “connection confirmed”.
- Delete the device in PaperCut by clicking “Delete this device” from the “Device Details” screen. Warning: This will also delete your settings for this device such as page cost settings.
- The device screen will go blank and show a message “Now remote operating.” Wait until it returns back to normal after 10-15 seconds, showing the standard copy settings screen.

In order to reactivate PaperCut functionality on the device, recommence installation as per the installation chapter of this document.

9 Known Limitations and Security

The Konica Minolta OpenAPI environment has a number of limitations that have an impact on functionality and security.

9.1 Combining Auto-color and Duplex

A duplex copy job with the “auto color” color setting that has mixed color and black-and-white pages will not differentiate between the color mode of the front and back side of a sheet. The color mode of both pages will be recorded as that of the front side.

9.2 Copy restrictions on restricted accounts

Users are prevented from logging in with a restricted account (user account or shared account) if another copy job charged to the same account is still in progress. Copy jobs in progress can be viewed using the “Job List” button on the device screen. Once the previous copy job has finished, users can log in again and charge to the restricted account. This behavior can be overridden using a configuration key, please see chapter 7.1.

9.3 PageScope Box Operator PC software

The PageScope Box Operator PC software is not designed to work with an MFD connected to an OpenAPI authentication application (like PaperCut). This is a limitation of the MFD and Box Operator software.

Users still have access to the Box Operator functionality via the devices web browser interface. It is recommended that users use this web interface instead of the PC software.

9.4 Job logging in case of network outages or firmware defects

PaperCut logs any user’s jobs after that user logs out, and the last job started during the session finishes. In case of network outages or device firmware defects, the log out may not have been reported to PaperCut by the device. PaperCut employs a number of timeout mechanisms to ensure jobs will still get logged eventually.

- After a delay of 1 hour (configurable, see section 7.1) of any user's inactivity, the user is assumed to have logged out and their jobs will be logged. Their funds, if escrowed, will also be made available and – in case of restricted users – logging in is allowed again.
 - Tracking log outs with early firmware releases of the A4 bizhub C35 model (mid-2011) has been shown to be more challenging than with A3 models. The escrow timeout therefore defaults to 10 minutes on those devices.
- After this delay of one hour, jobs being reported as finished by the device will still be logged by PaperCut, with a delay of 5 minutes (configurable, see section 7.1). An example for a job being started during a session and not completing before one hour later may be a job that has been paused due to paper outage.
- Jobs reported after more than 24 hours of one user's inactivity (configurable, see section 7.1) will not be logged or charged to any user.

9.5 Account Selection and Print Release

The authentication process may present an option to select a shared account and, if presented, will enforce that one account be selected. Copies produced will be charged to this shared account. However, print jobs released will remain unaffected by this choice and will be charged to the account selected when sending the print job.

9.6 Bypassing the System

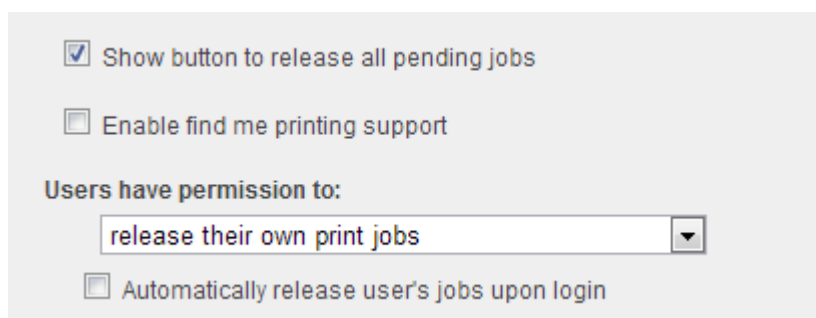
It is important that the administrators take care to prevent users from bypassing the system and directly accessing the copier. Likewise it is also important that administrators know how to bypass/disable the system if direct copier access is required – say to change advanced system settings. Administrations should take the following precautions:

The copier's administrator password should be changed and always kept secure.

9.7 Release All Device Configuration is Always Shown

The embedded solution supports making the "Print All" button that releases all jobs on the print release screen configurable. Administrators may take away this ability on a device.

Note that the option is shown even when operating with the non i-Option device/mode (where it is not supported).



The screenshot shows a configuration window with the following elements:

- ☒ Show button to release all pending jobs
- ☐ Enable find me printing support
- Users have permission to:
- (dropdown menu)
- ☐ Automatically release user's jobs upon login

9.8 Browser Resetting to the Connection Screen

After a period of inactivity on the MFD, the browser will restart and go to the PaperCut connection screen followed by the start screen, which varies depending on the device configuration in PaperCut.

The automatic reset behaviour is controlled by the device and is configurable using:

Administrator setting > Environment setting > Reset setting > Auto reset > Web browser.

Note that hitting “Reset” button on the panel will reset the browser to the initial screen so any screen currently shown will be navigated from and dismissed, this is not configurable.

9.9 Browser screen appears with scroll bars

The embedded software automatically detects maximum display panel resolution advertised by the device and runs at that resolution.

On some devices, a higher resolution value may be returned preventing the screen from being sized correctly and resulting in scroll bars appearing.

This makes the interface harder to use due to excessive scrolling, which can be rectified by manually overriding the configuration settings (`ext-device.konica-minolta.browser.screen-height` and `ext-device.konica-minolta.browser.screen-width`) until optimal resolution is achieved. See section 7.1.

9.10 Browser SSL Certificate Installation

The i-Option embedded application supports automatic installation of SSL certificates. This capability is only supported on OpenAPI 4.x devices, and works as follows:

- The certificate assigned to the PaperCut application server (that is the certificate used for the identity of the application server when SSL is enabled) is located and retrieved.
- The certificate will be automatically imported as trusted to the browser of the MFD.
- If the device doesn't support SSL certificate import and an SSL connection to the PaperCut application server is used together with the default self-signed certificate, then the browser may display warnings about the SSL connections (trust, hostname verification). In such cases the certificate may need to be manually installed by the administrator.
- Alternatively if you don't want to install certificate manually on all the devices – another option is to select 'Certificate Verification Settings' within the device web console (PageScope Web Connection), and set validation to 'OFF'.
- If a certificate issued by the standard issuing certificate authorities is used on the PaperCut application server, then the manual steps may not be needed (as the device browser comes with a set of 'standard' trusted certificates).

Example SSL warning dialog displayed by the NetFront browser:



9.11 Browser and connection errors

The browser that's installed on the MFD may show error pop-ups whenever any connectivity errors are detected between the browser and the application server. These are controlled by the browser and the device including any messages that are displayed.

When a pop-up dialog is displayed the device may switch away from the browser to the native user interface. After acknowledging the error dialog the switch back to the browser application is done. It is possible for switch back to not work correctly and either the browser interface not to be brought to the foreground automatically or a blank screen to be shown which can be rectified by hitting "Reset" key to reset the browser to the initial screen.

10 FAQ & Troubleshooting

The device screen is showing “Connecting to server ...” for an extended period

This message should not appear for more than a few seconds. If this message does not go away (or if it is followed by an error message) then this indicates a problem.

1. Is the device’s network connection functional?
2. Is there a useful error message displayed in the PaperCut admin interface at "Devices -> [device] -> Device status" (gray box)?
3. Try switching off the device for 5 seconds and switching it on again. This may resolve some network connectivity issues.
4. Can the device connect to the PaperCut server on port 9192? You may need to check routers and firewalls, including the Windows software firewall. A good way to test this is to telnet to the server’s IP address on port 9192 (`telnet 1.2.3.4 9192`).
5. Does the device have the latest firmware installed? Connection problems may occur with older firmware versions on some devices.
6. What is the IP address of the primary server? When starting the application server service, e.g. after a reboot or, in Windows, through Control Panel > Administrative Tools > Services > PaperCut Application Server, you will find a line like this in the log file [app-path]/server/logs/server.log:

```
# System details: max memory: 493.1 MB, processors: 2, free space: 119,516.8
MB, hostname: aragorn, IP addresses: [192.168.1.23,
fe80:0:0:0:d168:5b94:721c:19b3%10], runtime: 1.6.0_11-b03, time-zone:
Australia/Sydney, locale: en_AU, encoding: windows-1252
```

The first IP address in the list of "IP addresses: [...]" will be the one that the Konica Minolta device uses to contact the PaperCut server. If you want it to use another address, e.g. if you have multiple interfaces; please change the option "`system.network-address`" in the global config editor, which is in the administrator web interface on the “Options” tab under “Actions” on the left (not to be confused with the device-level config editor on the “Devices” tab).

When starting the device with no network connection the boot screen may be continuously displayed

Device may not discover an active network connection after a certain point and remain on Konica Minolta boot screen, possible remedy may be to hold the power button on the panel to trigger the “Sub Power Off” mode followed by turning it on and hitting ‘Access’ button.

Another alternative would be powering off and on using the main power switch.

The device screen is showing an error message “Your copy job has reached its maximum color/black & white allowance” although no user is currently accessing the device

This message appears when a user starts a copy job, walks away and at some point the copy job reaches its maximum allowance. The user that started the copy job or an administrator will have to log in to delete the job.

After restarting the MFP authentication/connectivity to PaperCut application server stops.

This problem may occur even if embedded was running successfully before the restart of the device. Repeating the embedded setup rectifies the problem temporarily until the reboot.

This may occur on some devices if SSDP network protocol is disabled. Even if not used it has to be enabled for the device to support integration with external authentication servers reliably.

I am seeing an error in the Device summary page that states “Error: login: error=12, message=no permission”

This message usually indicates that the credentials you’ve used to connect to the device are wrong. These credentials will be the same as the username and password you enter when logging into the admin UI of the device.

Warning appears on device summary page that states “The i-Option browser interface is not available.”

The warning appears if the target device is detected as supporting web browser functionality but it’s not been enabled in the configuration. The default (standard UI) interface is being used instead. Advanced device configuration key ext-device.konica-minolta.browser.enabled can be set to Y to enable i-Option (browser) interface. See Configuration Editor 7.1.

Standard Konica Minolta UI is shown instead of PaperCut’s web browser UI even though i-Option is setup.

Ensure the device has started successfully by checking device status window on the Device Details > Summary page.

Check that the browser interface is not disabled in PaperCut configuration under Device Details > Advanced Config tab under key ext-device.konica-minolta.browser.enabled (Y for browser/i-Option interface). See Configuration Editor 7.1.

If the configuration looks in order, this may mean that the setup process has determined that the browser functionality is not available on the device, please check you have browser license installed on the MFP and that you have obtained LK101 upgrade kit from Konica Minolta, Refer to setup procedure step 13.

Device displays continuously displays “Connecting” message but doesn’t connect to PaperCut application server.

The connecting screen is automatically rendered as the first screen on the device which immediately should proceed to the logon screen. The transition is done using JavaScript so if it’s disabled in the browser settings this will not occur. Please check the browser settings on the MFP and any relevant networking settings that may impede connectivity to PaperCut application server from the MFP. See 4.3.2

Setup of the Device fails, or subsequently shows an error “Device registered a fault or a component reached end of life”

Device cannot be managed and fails to register with the PaperCut App Server. Sometimes this issue stems from faults with the device or its attachments (for example a faulty feeder or filter).

As an example, this was seen with ozone filters reaching end of life status, or waste basket errors on the device.

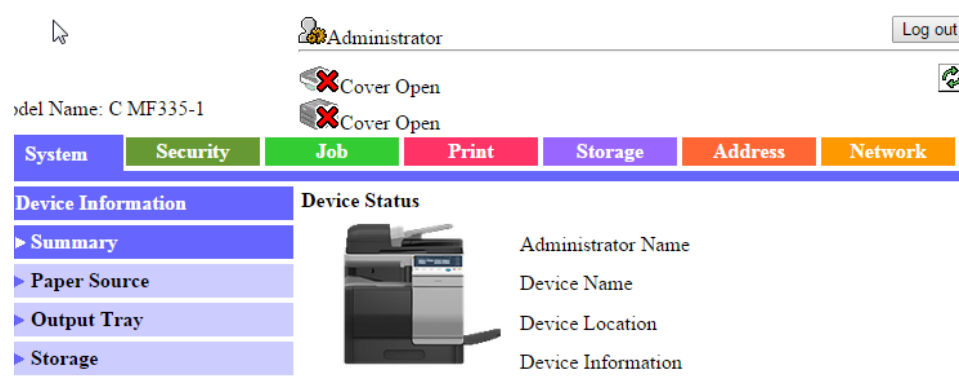
In some cases errors may not show up on the device itself, but normally the MFP returns an error in the PaperCut debug logs:

```
login: error=9, message=Error
```

```
login: error=9, message=Fatal
```

For example: "2015-03-09 06:59:37,088 ERROR KMEExtDevice:346 - login: error=9, message=Error [dev\konica552_workroom]"

Check if you can login in to the PageScope web connection console, and see if the copier icon shows up with an exclamation mark or a tool next to it with a flashing message/icon:



Ensure that the device error is rectified, and then try embedding the device with PaperCut again.

Browser gestures resize the authentication screen.

The web browser on the MFD used for hosting all of the UI supports gestures. The gestures such as “pinch in” or “pinch out” allow the window to be resized and content zoomed.

PaperCut integration instructs the MFP browser not to activate gestures in its own UI as this provides better user experience.

This feature is supported on some of the Minerva/Zeus series running (WebKit Browser Ver 1.4).

Long document and account names do not use ellipsis.

When running on device models that include NetFront browser any long document names or long account names may not include the terminating ellipsis suffix ‘...’ the values instead are simply truncated.

I am getting the following error message on device screen “Unable to unlock device for use, please try again.”

This message may intermittently be shown at the end of the login process into the MFD when done immediately after another user has logged out that had a job finishing at the time.

The error may occur intermittently anywhere between 10 seconds to a minute after the job has finished and another login has started.

When using scan to me (email) feature both from and to addresses are set to the user email address.

MFD allows the email address to be set for the machine under administrator settings, however when used together with the authentication application and personal sender is enabled (ext-device.konica-minolta.email.personalized-sender) the MFD automatically uses this address for both to and from fields in any emails.

If personal sender value is not set, the configured machine email address takes effect and is used as from field but scan to me function is not enabled by the device.

This is a known limitation of the OpenAPI platform.

When the UI is shown, a message is displayed: “Certificate credentials could not be verified”

This message is usually indicative of the MFD browser not having the certificate used by PaperCut application server in its trusted certificate store.

When managing the device using OpenAPI4 device type the certificate is usually automatically imported.

Depending on the type of browser installed on the device and the model/firmware it may be possible to manually import the certificate.

In the case of models using NetFront browser, the certificate can be manually imported by logging to the device as administrator and starting the browser manually then importing the certificate via the browser UI (URLInput button).

Normally in this case the certificate needs to be extracted out of PaperCut and hosted on any web server that can be accessed from the MFD. A URL to the hosted certificate is used to import the certificate into the browser.

Alternatively, it may be possible to turn the certificate validation off by logging in as administrator, starting the browser and changing the option under the security tab. This option is available on some builds of WebKit browser embedded on the MFD.

I've plugged the card reader in but it doesn't seem to activate the copier?

The MFDs often have multiple USB ports. Some are suitable for use with a card reader, some are not. Please ensure that you have tried all the USB ports on the machine.

Can I disable the logout confirmation?

The logout confirmation screen is controlled by the copier and can be configured via Utility -> Administrator Settings -> User Authentication/Account Track -> User/Account Common Setting -> Logout Confirmation Screen Display Setting.

Why is the on screen keyboard missing some characters, e.g. the "@" symbol

The locale and / or language of the keyboard and copier can change the selection of characters available on the on screen keyboard. You may need to select another language and / or locale to obtain characters commonly used in your organisation.

To use locale specific symbols the keyboard type may need to be set to "Local Keyboard" in the panel utility menu. This is set under Utility > User Settings > System Settings > Select Keyboard.

